International Journal of Electronics and Communication Engineering (IJECE)
ISSN(P): 2278-9901; ISSN(E): 2278-991X
Vol. 3, Issue 2, Mar 2014, 49-58

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

DYNAMIC CERTIFICATION AUTHORITY BASED MANETs

VIJENDER SINGH HOODA[1] & AMNINDER KAUR[2]

[1]Research Scholar, Associate Professor, Department of Information & Technology, Dronacharya College of Engineering, Gurgaon, Haryana, India

[2]Associate Professor, Department of Electronics & Communication Engineering, Dronacharya College of Engineering, Gurgaon, Haryana, India

ABSTRACT

Ad hoc network security has been considered as most significant research topic in recent time. Authentication and trust management in an ad hoc network is a challenging task now days. In order to provide security mechanisms that are based on public key technology, it is necessary to create the supporting key management infrastructure, which is commonly uses the concept of a certificate authority (CA). For public key based security services, establishing a CA can be cause of great difficulty without a trusted authority and global centralized and. The exclusive characteristics of mobile ad hoc networks causes a number of nontrivial challenges to design a security architecture such as open network architecture, shared wireless medium, stringent resource constraints and highly dynamic topology in distributes systems. In MANET any node may compromise the packet routing functionality by disrupting the route discovery process. A Distributed Certificate Authority (DCA) is realized through the distribution of the CA's private key to a number of special shareholding DCA nodes. When CA- related operations are required, such as issuing or signing a certificate, checking public keys, or revoking certificates, a threshold of available shareholding DCA nodes should participate in the operation. There has been relatively slight work to date on designing distributed CA services. This paper proposes a new model for a distributed certificate authority in NTDR (Near-Term Digital Radio cluster-based ad hoc networks. The DCA's private key is never known by any single node, either during setup or during certificate authority-related operations.

KEYWORDS: Ad-hoc Network, Certificate Authority CA, Distributed Certificate Authority (DCA), Security

1. INTRODUCTION

Security in mobile ad-hoc networks is hard to achieve due to dynamically changing and fully decentralized topology as well as vulnerability and scarcity of wireless link. Wireless networks consist of a number of nodes which communicate with each other over a wireless channel which have various types of networks: sensor network, ad hoc mobile networks, wireless networks, cellular networks and satellite networks [1]. Wireless sensor networks consist of small nodes with sensing, computation and wireless communications capabilities. Many routing protocols have been specifically designed for WSNs where energy awareness is the key issue. Routing protocols in WSNs differ depending on the application and network architecture [2]. Ad-hoc networks are a new paradigm of wireless communication for mobile hosts where node mobility causes frequent changes in topology. Ad hoc networks are self-configurable and autonomous systems consisting of routers and hosts, which are able to support movably and organize themselves arbitrarily. This means that the topology of the ad hoc network changes dynamically and unpredictably. In Mobile Ad hoc Networks, there will not be any centralized coordinator like base stations and also the availability of the limited resources makes Quality of Service a

Challenging Issue. To sort out such issues DCA has been introduced. To establish a distributed rating system two sub-problems have to be solved, which are: a) the detection of an attacker, and b) the revealing of this information to the ad-hoc community. The process of information revelation requires that the system support at least the mechanism of non repudiation. Since all nodes are mobile; the network topology of a MANET is generally dynamic and it may change frequently according to the scenario. Thus, protocol such as 802.11 to communicate via same frequency or Bluetooth have require power consumption is directly proportional to the distance between hosts, direct single-hop transmissions between two hosts can require significant power, causing interference with other such transmissions. To avoid this routing problem, two hosts can use multi-hop transmission to communicate via other hosts in the network. A router should provide the ability to rank routing information sources from most trustworthy to least trustworthy and to accept routing information about any particular destination from the most trustworthy sources first.

A router should provide a method to filter out obviously invalid routes. Routers must not by default redistributes routing data they do not themselves use, trust or otherwise consider valid. Routers must be at least a little paranoid about accepting routing data from anyone, and must be especially careful when they distribute routing information provided to them by another party [3].

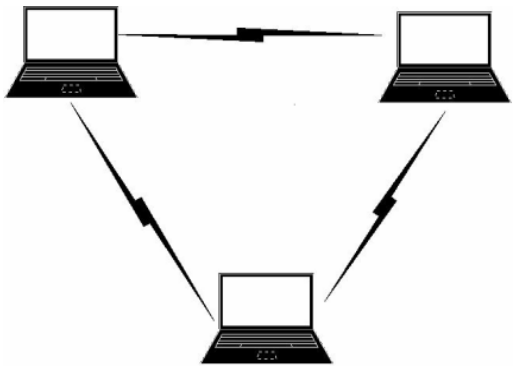

Figure 1: Ad-hoc Network

Figure 1 shows three nodes where ad hoc network where every node is connected to wireless, and work as access point to forward and receive data. This article discusses attacks on ad hoc networks and discusses current approaches for establishing cryptographic keys in ad hoc networks. We describe the state of research in secure ad hoc routing protocols, routing challenges and its research issues.

2. SECURITY CHALLENGES IN ADHOC NETWORKS

Use of wireless links renders an Ad hoc network susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay and message distortion [4]. Eavesdropping might give an attacker access to secret information thus violating confidentiality. Active attacks could range from deleting messages, injecting erroneous messages; impersonate a node etc thus violating availability, integrity, authentication and non repudiation. Nodes roaming freely in a hostile environment with relatively poor physical protection have non-negligible probability of being compromised. Hence, we need to consider malicious attacks not only from outside but also from within the network from compromised nodes. Thus following are the ways by which security can be breached [5].

- **Vulnerability of Channels:** As in any wireless network, messages can be eavesdropped and fake messages can be injected into the network without the difficulty of having physical access to network components.

- **Vulnerability of Nodes:** Since the network nodes usually do not reside in physically protected places, such as locked rooms, they can more easily be captured and fall under the control of an attacker.
- **Absence of Infrastructure:** Ad hoc networks are supposed to operate independently of any fixed infrastructure. This makes the classical security solutions based on certification authorities and on- line servers inapplicable [6].
- **Dynamically Changing Topology:** In mobile ad hoc networks, the permanent changes of topology require sophisticated routing protocols, the security of which is an additional challenge. A particular difficulty is that incorrect routing information can be generated by compromised nodes or as a result of some topology changes and it is hard to distinguish between the two cases.

For high survivability Ad hoc networks should have a distributed architecture with no central entities, centrality increases vulnerability. Ad-hoc network is dynamic due to frequent changes in topology.

3. SECURITY MODEL

In this section we first discuss security goals attacks and thus secure routing protocols which are following:

3.1 Security Goals for Ad-hoc Networks

- **Availability:** Ensures survivability despite Denial of Service (DOS) attacks. On physical and media access control layer attacker can use jamming techniques to interfere with communication on physical channel. On network layer the attacker can disrupt the routing protocol. On higher layers, the attacker could bring down high level services e.g.: key management service.
- **Confidentiality:** Ensures the robustness of information as it is never disclosed to unauthorized entities.
- **Integrity:** Message being transmitted is never get any error.
- **Authentication:** Enables it provides the identity of peer node through which it is communicating. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes [7].
- **Non-Repudiation:** It ensures that the origin of a message cannot deny having sent the message.
- **Non-Impersonation:** No one else can pretend to be another authorized member to learn any useful information.
- **Attacks Using Fabrication:** Generation of false routing messages is termed as fabrication messages. Such attacks are difficult to detect [8].

3.2 Attacks on Ad hoc Network

Ad Hoc Network provides the dynamic authentication. So its very common practice to search the loop holes and attack on Ad Hoc networks. Here different types of attacks are listed below:

- **Location Disclosure:** Location disclosure is an attack that targets the privacy requirements of an ad hoc network. Through the use of traffic analysis techniques [9], or with simpler probing and monitoring approaches, an attacker is able to discover the location of a node, or even the structure of the entire network.

- **Black Hole:** In a black hole attack a malicious node injects false route replies to the route requests it receives, advertising itself as having the shortest path to a destination These fake replies can be fabricated to divert network traffic through the malicious node for eavesdropping, or simply to attract all traffic to it in order to perform a denial of service attack by dropping the received packets.
- **Replay:** An attacker that performs a replay attack injects into the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions.
- **Wormhole:** The wormhole attack is one of the most powerful presented here since it involves the cooperation between two malicious nodes that participate in the network [10].
- **One Attacker:** e.g. node A, captures routing traffic at one point of the network and tunnels them to another point in the network, to node B, for example, that shares a private communication link with A. Node B then selectively injects tunneled traffic back into the network. The connectivity of the nodes that have established routes over the wormhole link is completely under the control of the two colluding attackers. The solution to the wormhole attack is *packet leashes*.
- **Blackmail:** This attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the offender [11]. An attacker may fabricate such reporting messages and try to isolate legitimate nodes from the network. The security property of non- repudiation can prove to be useful in such cases since it binds a node to the messages it generated.
- **Denial of Service:** Denial of service attacks aim at the complete disruption of the routing function and therefore the entire operation of the ad hoc network. Specific instances of denial of service attacks include the routing table overflow and the sleep deprivation torture. In a routing table overflow attack the malicious node floods the network with bogus route creation packets in order to consume the resources of the participating nodes and disrupt the establishment of legitimate routes. The sleep deprivation torture attack aims at the consumption of batteries of a specific node by constantly keeping it engaged in routing decisions.
- **Routing Table Poisoning:** Routing protocols maintain tables that hold information regarding routes of the network. In poisoning attacks the malicious nodes generate and send fabricated signaling traffic, or modify legitimate messages from other nodes, in order to create false entries in the tables of the participating nodes [12]. For example, an attacker can send routing updates that do not correspond to actual changes in the topology of the ad hoc network. Routing table poisoning attacks can result in the selection of non-optimal routes, the creation of routing loops, bottlenecks, and even portioning certain parts of the network.
- **Rushing Attack:** Rushing attack is that results in denial-of-service when used against *all* previous on-demand ad hoc network routing protocols. For example, DSR, AODV, and secure protocols based on them, such as Ariadne, ARAN, and SAODV, are unable to discover routes longer than two hops when subject to this attack. develop *Rushing Attack Prevention (RAP)*, a generic defense against the rushing attack for on-demand protocols that can be applied to any existing on-demand routing protocol to allow that protocol to resist the rushing attack.
- **Masquerading:** During the neighbor acquisition process, an outside intruder could masqueraded a nonexistent or

existing IS by attaching itself to communication link and illegally joining in the routing protocol domain by compromising authentication system.

- **Breaking the Neighbor Relationship:** An intelligent filter is placed by an intruder on a communication link between two ISs(Information system) could modify or change information in the routing updates or even intercept traffic belonging to any data session.
- The threat of masquerading is almost the same as that of a compromised IS.
- **Passive Listening and Traffic Analysis:** The intruder could passively gather exposed routing information. Such an attack can not affect the operation of routing protocol, but it is a breach of user trust to routing the protocol. Thus, sensitive routing information should be protected. However, the confidentiality of user data is not the responsibility of routing protocol.

4. MANET MODEL

A mobile ad hoc network is a group of wireless nodes that can dynamically be set up anywhere and anytime without using any pre-existing network infrastructure [13]. It is an autonomous system in which mobile hosts connected by wireless links are free to move randomly and often act as routers at the same time. The traffic types in ad hoc networks are quite different from those in an infrastructure wireless network, including:

- **Peer-to-Peer:** Communication between two nodes which are within one hop. Network traffic (Bps) is usually consistent.
- **Remote-to-Remote:** Communication between two nodes beyond a single hop but which maintain a stable route between them. This may be the result of several nodes staying within communication range of each other in a single area or possibly moving as a group. The traffic is similar to standard network traffic.
- **Dynamic Traffic:** This occurs when nodes are dynamic and moving around. Routes must be reconstructed. This results in a poor connectivity and network activity in short bursts.

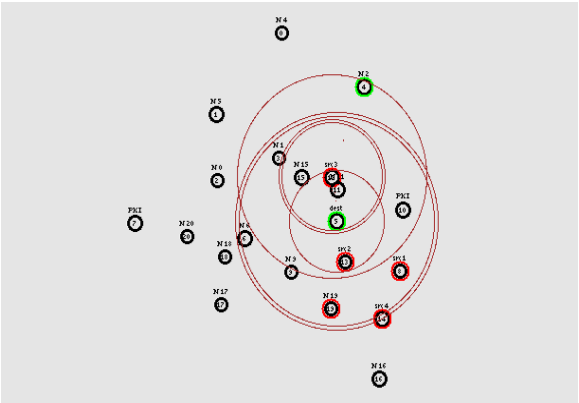

Figure 2: Node MANET

4.1 MANET Condition

Ad hoc networking is not a new technique which comes recently in the communication world. As a technology for dynamic wireless networks, it has been deployed in military since 1970s. Commercial interest in such networks has

recently grown due to the advances in wireless communications. A new working group for MANET has been formed within the Internet Engineering Task Force (IETF) [14], aiming to investigate and develop candidate standard Internet routing support for mobile, wireless IP autonomous segments and develop a framework for running IP based protocols in ad hoc networks. The recent IEEE standard 802.11 has increased the research interest in the field. Many international conferences and workshops have been held by e.g. IEEE and ACM. For instance, MobiHoc (The ACM Symposium on Mobile Ad Hoc Networking & Computing) has been one of the most important conferences of ACM SIGMOBILE (Special Interest Group on Mobility of Systems, Users, Data and Computing). Research in the area of ad hoc networking is receiving more attention from academia, industry, and government. Since these networks pose many complex issues, there are many open problems for research and significant contributions.

4.2 MANET Features

MANET has the following features:

- **Autonomous Termina:** In MANET, each mobile terminal is an autonomous node, which may mobile nodes can also perform switching functions as a router. So usually endpoints and function as both a host and a router. In other words, besides the basic processing ability as a host, the switches are indistinguishable in MANET.
- **Distributed Operation:** Since there is no background network for the central control of the network operations, the control and management of the network is distributed among the terminals. The nodes involved in a MANET should collaborate amongst and each node acts as a relay as needed, to implement functions e.g. security and routing [15].
- **Multihop Routing:** Basic types of adhoc routing algorithms can be single-hop and multihop, based on different link layer attributes and routing protocols. Single-hop MANET is simpler than multihop in terms of structure and implementation, with the cost of lesser functionality and applicability. When delivering data packets from a source to its destination out of the direct wireless transmission range, the packets should be forwarded via one or more intermediate nodes.
- **Dynamic Network Topology:** Since the nodes are mobile, the network topology may change rapidly and unpredictably and the connectivity among the terminals may vary with time. MANET should adapt to the traffic and propagation conditions as well as the mobility patterns of the mobile network nodes. The mobile nodes in the network dynamically establish routing among themselves as they move about, forming their own network on the fly. Moreover, a user in the MANET may not only operate within the ad hoc network, but may require access to a public fixed network (e.g. Internet).
    - Infrastructure-based wireless network
    - Ad hoc wireless network
- **Fluctuating Link Capacity:** The nature of high bit-error rates of wireless connection might be more profound in a MANET. One end-to-end path can be shared by several sessions. The channel over which the terminals communicate is subject to noise, fading, and interference, and has less bandwidth than a wired network. In some scenarios, the path between any pair of users can traverse multiple wireless links and the link themselves can be heterogeneous [16].

- **Light-Weight Terminal:** In most cases, the MANET nodes are mobile devices with less CPU processing capability, small memory size, and low power storage. Such devices need optimized algorithms and mechanisms that implement the computing and communicating functions.

4.3 Challenges in MANET

Regardless of the attractive applications, the features of MANET introduce several challenges that must be studied carefully before a wide commercial deployment can be expected. These include:

- **Routing:** Routing is the biggest challenge for MANET. Since the topology of the network is constantly changing, the issue of routing packets between any pair of nodes becomes a challenging task. Most protocols should be based on reactive routing instead of proactive. Multicast routing is another challenge because the multicast tree is no longer static due to the random movement of nodes within the network. Routes between nodes may potentially contain multiple hops, which is more complex than the single hop communication.
- **Security and Reliability:** In addition to the common vulnerabilities of wireless connection, an ad hoc network has its particular security problems due to e.g. nasty neighbor relaying packets. The feature of distributed operation requires different schemes of authentication and key management. Further, wireless link characteristics introduce also reliability problems, because of the limited wireless transmission range, the broadcast nature of the wireless medium (e.g. hidden terminal problem), mobility-induced packet losses, and data transmission errors.
- **Quality of Service (QoS):** Providing different quality of service levels in a constantly changing environment will be a challenge. The inherent stochastic feature of communications quality in a MANET makes it difficult to offer fixed guarantees on the services offered to a device. An adaptive QoS must be implemented over the traditional resource reservation to support the multimedia services.
- **Power Consumption:** For most of the light- weight mobile terminals, the communication- related functions should be optimized for lean power consumption. Conservation of power and power-aware routing must be taken into consideration [17].
- **Internetworking:** In addition to the communication within an ad hoc network, internetworking between MANET and fixed networks (mainly IP based) is often expected in many cases. The coexistence of routing protocols in such a mobile device is a challenge for the harmonious mobility management

5. DISTRIBUTED CERTIFICATE AUTHORITY

The increasing interest in ad hoc networks has made their security a real concern. As a result, ad hoc network security has been subject to extensive recent study. While much attention has been spent looking at security of routing protocols in ad hoc networks, for example it is equally important to secure communications in ad hoc networks [18]. In order to employ security mechanisms that are based on public key technology, it is necessary to establish the supporting key management infrastructure, which is normally based around the concept of a *certificate authority* (CA).However security in mobile ad hoc networks is particularly challenging for many reasons, including the dynamically changing topology; the sporadic nature of connectivity ; the vulnerability of link of links; the limited physical protection of nodes; The lack of centralized monitoring or management points. The latter is arguably the most crucial for offering public key based security services because, in the absence of a global centralized and trusted authority, establishing a CA can be

highly problematic, if not impossible. An attractive idea is thus to distribute a CA's functionality amongst ad hoc network nodes. A *Distributed Certificate Authority (DCA)* is realized through the distribution of the CA's private key to a number of special *shareholding* DCA nodes.

When CA-related operations are required, such as issuing or signing a certificate, checking public keys, or revoking certificates, a threshold of available shareholding DCA nodes should participate in the operation. There has been relatively little work to date on designing distributed CA services (we will discuss related work in Section 4). In this paper we present a new model for a distributed certificate authority in NTDR (Near-Term Digital Radio [19]) cluster-based ad hoc networks. The DCA's private key is never known by any single node, either during setup or during certificate authority-related operations.

5.1 Design Goals

Desirable design properties for a scalable DCA are as follows:

- **Availability:** Nodes may seek a DCA' services at any time and require a response within a reasonable delay period. However, a solution must take into account the dynamic nature of an ad hoc environment. It can be expected that not every shareholding DCA node is reachable at any given time and, further, that the collection of shareholding DCA nodes varies over time. We thus require protocols to enable shareholding DCA nodes to leave and join the DCA.
- **Security:** Since nodes may fall victim to different types of attack (for instance, capture); no important system secret values are to be trusted to any single node in the network. Thus, for example, DCA key pairs must be generated in a distributed way and the DCA private key should be usable without any single shareholding DCA node being able to reconstruct it. In addition, a key refresh protocol is required to ensure that the lifetimes of critical keys are restricted.
- **Reliability:** Wherever possible, the system should avoid relying solely on the underlying communication network, since channels or nodes could be compromised. Where possible, measures should be taken to improve system robustness.
- **Efficiency:** As nodes are power-limited and communication bandwidth is relatively low, protocols should attempt to minimize computations, connections and the amount of data transmitted between nodes [20].

5.2 DCA Security Services

The purpose of having a DCA in an NTDR network is to make use of public key-based cryptographic services. These services include support for authentication, integrity, confidentiality, access control and non-repudiation. These are required between nodes, between nodes and cluster heads, and between cluster heads. Public key techniques are attractive because they enable nodes to establish secure links without having prior relationships. However public key techniques are generally computationally intensive and so the application of public key cryptography in the NTDR security framework is largely restricted to initial node authentication and key establishment processes. Public key cryptography involves two related keys, one of which is private and the other public. It is essential that the authenticity and validity of public keys is maintained, and the normal means of doing so is for a trusted entity (in our case the DCA) to issue a *public key certificate* attesting to this information.

The DCA provides all public key certificate services, in particular issuing, revocation, renewing, and verification of certificates. When a new node first joins the NTDR network, it presents its offline certificate to the cluster head with which it intends to affiliate. It should then seek an *on-line certificate* from the DCA, which is then used as the working certificate in the NTDR network [21].

5.3 DCA Architecture

It is entirely natural that we propose that our DCA is distributed amongst cluster heads, which become the shareholding DCA nodes. This is because cluster heads hold positions of responsibility in the NTDR network and are in direct communication with one another, making them the most appropriate nodes to fulfill this role. The DCA private key must therefore be distributed and maintained amongst the cluster heads [22]. When a new cluster head joins the backbone they need to be issued with a share of the DCA private key. When a node seeks a DCA services (such as a certificate renewal), the node first contacts their cluster head who then takes up the request with the other cluster heads.

We will define our DCA by specifying the following DCA operations:

- System setup or bootstrapping,
- Applying a DCA private key,
- Joining a new cluster head,
- Evicting an existing cluster head,
- Refreshing cluster head shares.

6. CONCLUSIONS

In this paper, the extended purpose of having a DCA in an NTDR network is to make use of public key- based cryptographic services. These services include support for integrity, confidentiality, authentication, access control, and non- repudiation. These are required between nodes, between nodes and cluster heads, and between cluster heads. This technique is also extended for distributed authority. Public key techniques are attractive because they enable nodes to establish secure links without having prior relationships. The application of public key cryptography in the NTDR security framework is largely restricted to initial node authentication and key establishment processes. The DCA provides all public key certificate services, in particular issuing, revocation, renewing, and verification of certificates. When a new node first joins the NTDR network, it presents its offline certificate to the cluster head with which it intends to affiliate. It should then seek an *on-line certificate* from the DCA, which is then used as the working certificate in the NTDR network. It is entirely natural that we propose that our DCA is distributed amongst cluster heads, which become the shareholding DCA nodes.

REFERENCES

1. Wong, C., Gouda, M., and Lam, S. Secure Group Communications Using Key Graphs. In Proceedings of the ACM SIGCOMM ’98 conference on Applications, technologies, architectures, and protocols for computer communication, pp. 68–79 (1998).
2. Shamir, A. How to Share a Secret. Communications ACM 1979; 22(11), pp. 612–613 (1979).

3. Tanenbaum, A. Computer Networks, PH PTR (2003).
4. M. Ilyas. The Handbook of Ad Hoc Wireless Networks, CRC Press, (2003).
5. Yi, S. and Kravets, R. Composite Challenges and Solutions. IEEE Wireless Communications, pp. 38- 47. (2004)
6. Yang, H., Luo, H., Ye, F., Lu, S., and Zhang, L. Security in Mobile Ad Hoc Networks, (2004).
7. Nichols, R., and Lekkas, P. Wireless Security-Models, Threats, and Solutions, McGraw Hill, Chapter 7. (2002).
8. Oppliger, R. Internet and Intranet Security, Artech House (1998).
9. Wu, B., Wu, J., Fernandez, E., Ilyas, M., and Magliveras, S. Secure and Efficient Key Management Scheme in Mobile Ad Hoc Networks. Journal of Network and Computer Applications (JCNA) (2005).
10. Wu, B., Wu, J., Fernandez, E., Magliveras, S., and Ilyas, M.Secure and Efficient Key Management in Mobile Ad Hoc Networks. Proc. Of 19th IEEE International Parallel & Distributed Processing Symposium, Denver (2005).
11. Zhou, L., and Haas, Z. Securing Ad Hoc Networks, IEEE Network Magazine vol.13, no. 6, pp.24-30 (1999).
12. Murthy, C., and Manoj, B. Ad Hoc Wireless Networks: Architectures and Protocols, Prentice Hall PTR (2005). .
13. Hubaux, J., Buttyan, L., and Capkun, S. .The Quest for Security in Mobile Ad Hoc Networks, In Proc. of the ACM Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc 2001).
14. M.S. Corson, J.P. Maker, and J.H. Cernicione, Internet-based Mobile Ad Hoc Networking, *IEEE Internet Computing*, pages 63–70, July-Augus (1999).
15. Yongguang Zhang and Wenke Lee, Security in Mobile Ad-Hoc Networks, in Book *AdHoc Networks Technologies and Protocols (Chapter 9)*, Springer, (2005).
16. L. Venkatraman and D. Agrawal, "A Novel Authentication Scheme for Ad Hoc Networks," in Proceedings of Wireless Communications and Networking Confernce, (2000).
17. J.-P. Hubaux, L. Buttyan, **S.** Capkun, 'The Quest for Security in Mobile Ad Hoc Networks," Proceedings of the ACM Symposium on Mobile Ad Hoc Networking.
18. P. Papadimitratos and Z. J. Hass, Secure Routing for Mobile Ad Hoc Networks, in Proceedings of *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS)*, San Antonio, TX, January (2002).
19. K. Sanzgiri, B. Dahill, B. Levine, C. Shields, E. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks", In Proceedings of IEEE International Conference on Network Protocols (ICNP), November (2002).
20. S. Yi and R. Kravets. MOCA: Mobile certificate authority for wireless ad hoc networks. In 2nd Annual PKI Research Workshop (PKI03), April (2003).
21. NS-2 (The Network Simulator). http://www.isi. edu/nsnam/ns/.